AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT
for the
MIDDLE DISTRICT OF PENNSYLVANIA

In the Matter of the Search of	
(Briefly describe the property to be searched or identify the person by name or address)	)))
INFORMATION ASSOCIATED WITH MATTEWW10@ICLOUD.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.	)))) Case No. 1:20-MC-00570

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the   SOUTHERN   District of CALIFORNIA

(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A. This court has authority to issue this warrant under 18 U.S.C. 2703 (c)(1)(A) and 2711(3)(A), as this court has "jurisdiction over the offense under investigation," and Fed.R.Crim.P.41. Because the government has satisfied the requirements of 18 U.S.C. 3122, this warrant also constitutes an order under 18 U.S.C. 3123.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

YOU ARE COMMANDED to execute this warrant on or before for 30 days   *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10 p.m.   ☑ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to
Hon. Susan E. Schwab
_____
(United States Magistrate Judge)

☑ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☑ for 30 ____ days *(not to exceed 30)*   ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 10/22/20 @ 3:47pm   *[signature]*
_____   _____
                                                            Judge's signature

City and state: HARRISBURG, PA   SUSAN E. SCHWAB, CHIEF MAGISTRATE JUDGE
_____   _____
                                                            Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

This warrant applies to information associated with Apple iCloud
account matteww10@icloud.com (the "account") that is stored at
premises owned, maintained, controlled, or operated by Apple Inc., a
company headquartered at Apple Inc., 1 Infinite Loop, Cupertino,
California 95014.

ATTACHMENT B

Particular Things to be Seized

I.   Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a.   All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status,

methods of connecting, and means and source of payment (including any credit or bank account numbers);

b.   All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c.   The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at

which each email was sent, the size and length of each email, and the

true and accurate header information including the actual IP addresses

of the sender and the recipient of the emails, and all attachments;

d.   The contents of all instant messages associated with the

account, including stored or preserved copies of instant messages

(including iMessages, SMS messages, and MMS messages) sent to and

from the account (including all draft and deleted messages), the source

and destination account or phone number associated with each instant

message, the date and time at which each instant message was sent,

the size and length of each instant message, the actual IP addresses of

the sender and the recipient of each instant message, and the media, if

any, attached to each instant message;

e.   The contents of all files and other records stored on iCloud,

including all iOS device backups, all Apple and third-party app data

(including, but not limited to WhatsApp and WeChat electronic, audio,

video, and picture communications), all files and other records related

to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo

Library, iCloud Drive, iWorks (including Pages, Numbers, and

Keynote), iCloud Tabs, and iCloud Keychain, and all address books,

contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f.   All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g.   All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h.   All records pertaining to the types of service used;

i.   All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j.   All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).